palgrave communications
HUMANITIES | SOCIAL SCIENCES | BUSINESS

COMMENT

Received 6 Jul 2016 | Accepted 30 Nov 2016 | Published 10 Jan 2017

DOI: 10.1057/palcomms.2016.102 OPEN

Cyberweapons: an emerging global governance architecture

Tim Stevens[1]

ABSTRACT Cyberweapons are a relatively new addition to the toolbox of contemporary conflict but have the potential to destabilize international relations. Since Stuxnet (a malicious computer worm) in 2010 demonstrated how computer code could be weaponised to generate political effect, cyberweapons have increasingly been discussed in terms of potential regulation and prohibition. Most analyses focus on how global institutions and regimes might be developed to regulate the development and use of cyberweapons and identify the political and technical obstacles to fulfilling this ambition. This focus on centralized authority obscures identification of existing governance efforts in this field, which together constitute an emerging global governance architecture for offensive cyber capabilities. This article explores three sources of cyberweapons governance—cyberwarfare, cybercrime and export controls on dual-use technologies—and briefly describes their political dynamics and prospects. It is argued that although fragmented, the global governance of cyberweapons should not be dismissed on this basis. Fragmentation is a condition of global governance, not its antithesis, and policy should respect this fragmentation instead of regarding it as an impediment to further development of cyberweapons governance. This article is published as part of a collection on global governance.

[1] King's College London, London, UK Correspondence: (e-mail: tim.stevens@kcl.ac.uk)

Introduction

Cyberweapons have been covert military and intelligence tools since the 1990s but it was only in 2010 that the strategic potential of weaponised code was put under the global spotlight. The disclosure by technical experts and journalists of a cyberweapon dubbed "Stuxnet" showed how computer code could be weaponised to generate political effect. Reportedly the product of a highly-classified US-Israeli intelligence programme, Stuxnet infiltrated the control systems of an Iranian nuclear facility to subvert its uranium enrichment operations (Sanger, 2012: 188–225; Zetter, 2014). It succeeded in doing so and, although its impact on the Iranian nuclear programme is probably overstated (Barzashka, 2013), it demonstrated that cyberweapons could be deployed as political weapons in pursuit of national interests. Stuxnet has also reopened older debates about how, and if, the acquisition and use of cyberweapons should be regulated or even prohibited, through institutions like "cyber arms control" regimes and conventions. This work suggests that obstacles to building such institutions are significant and possibly counter-productive and perhaps should not be attempted in the first place. The continued focus on centralized mechanisms has prevented a clear assessment of extant or emerging measures regulating the acquisition and use of cyberweapons in peace and war. This commentary proposes that global governance is a more appropriate lens through which to view these processes and that a nascent global governance architecture for cyberweapons already exists.

The argument proceeds as follows. The first section defines and describes what is meant by "cyberweapon", a term often used loosely and without analytical rigour. This is followed by a brief review of previous arguments relating to the regulation of cyberweapons and why "global governance" is a more useful perspective than a focus on regimes alone. Cyberwarfare, cybercrime and export controls on dual-use technologies are then explored to show how global governance in the absence of centralized authority is emerging, albeit slowly and in disjointed fashion. The final section analyses this governance architecture, concluding that, whilst fragmented, this should be seen as a condition of cyberweapons governance, not as an excuse for failure or inaction.

Cyberweapons

"Cyberweapon" has become a catch-all term for diverse forms of malicious software (malware) for which an extraordinary range of capabilities is claimed. Cyberweapons are conceived on a spectrum from low-level internet irritants, to war-winning "cyber bombs", even to the equivalents of "weapons of mass destruction". The reality is rather less dramatic and the term—if it is to be used at all (Valeriano *et al.*, 2016)—has been defined as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings" (Rid and McBurney, 2012; Rid, 2013: 37). This is broadly analogous to established notions of a weapon as "an offensive capability that is applied, or that is intended or designed to be applied, to an adversary to cause death, injury or damage" (Boothby, 2016: 166). However, these are not juridical or legal terms, as there is no consensus definition of either weapons or cyberweapons in international law. For our purposes, it is sufficient that a weapon meets the criteria of intentionality and harm, although cyberweapons present at least two additional challenges to definition and conceptualization.

The first is that most cyberweapons lack conventional physicality: they are computer code that exists only in information infrastructures like the internet. They are "in the world but not experienced as part of the world" (Floridi, 2014: 318), until such time as their effects manifest in more conventional ways. The existence, operations and effects of cyberweapons and other "information objects" are wholly contingent on physical processes, entities and events (Dipert, 2014: 36–37), but cyberweapons are not themselves physical in any natively comprehensible fashion. This is significant, not only as this makes them difficult to track and interdict, but because most jurisdictions and legal regimes understand weapons to be material, rather than immaterial, entities (Mele, 2013: 9). The exception to this is when modified hardware is used as a cyberweapon, or when hardware is specifically designed to be part of a cyber weapons system (Schmitt, 2013: 142), both of which should be considered alongside cyberweapons *qua* informational objects.

The second is the nature of harm. Moral arguments as to the nature of harm—most notably in the liberal tradition (Linklater, 2006)—do not consider harm to non-humans, so the extension of the concept of harm to "structures, systems, or living beings" (Rid, 2013: 37) is philosophically problematic (also, Arimatsu, 2012: 97). "Harm" in this context must include the related concepts of "damage" or "impairment", which do apply to non-humans and non-sentient systems. In a slightly metaphorical register, therefore, this expansive category of harm covers outcomes injurious to the well-being of a target system, or which set back the interests of that system. For example, malware that extracts data but does not use it to degrade or subvert a computer system would not be considered a cyberweapon (Rid, 2013: 47). However, as establishing the nature and degree of harm is a notoriously subjective process, it is difficult to develop precise thresholds for what constitutes harm or otherwise, not least as the type and severity of harm depends on the nature of the target. Notwithstanding the issue of whether non-cognising entities can experience harm, this points to the relational nature of harm. Cyber weapons are not equipped with "an explosive charge", so harm is caused by altering processes of the targeted system, rather than as a direct result of some innate attribute of weaponised code (Rid, 2013: 41). This applies to the logical functioning of a targeted computer system, which is affected directly by a cyber weapon, and to the second-order effects of cyber weaponry, such as financial loss or reputational damage to a company subject caused by a cyber attack. It should also include the affective implications of the use of cyber weapons (Stevens, 2016a: 103–104) if they result in harm, perceived or actual, to human subjects. These might include feelings of insecurity or fear caused by infrastructure failure, or the more mundane but no less real emotions that result from personal data loss. In both cases, these are usually indirect weapons effects (Rid, 2013: 40), although, *contra* Rid, this does not necessarily alter the original code's intended status as a weapon.

One further comment is necessary on the identification of software as a weapon. As the above discussion affirms, weapons are not technical artefacts alone but hybrid assemblages of human and non-human entities (Bourne, 2012). The appeals to harm and intent reflect this concern with human agency as the principal determinant of "weapon-ness" throughout the various stages of planning, design, development and deployment, as well as in mechanisms of commercial and criminal exchange. Nevertheless, the construction of malware as weapons may on occasion hinder rather than help understanding of these complex entities. This operates, first, by conflating disparate tools and instruments within a single rubric and, second, by masking the heterogeneity of their anatomies and deployments within a field of militarized discursivity. As we will encounter below in the discussion of dual-use technologies, many "cyberweapons" have defensive rather than offensive purposes, and, far from being intended to cause harm, can be used for socially beneficial reasons. In that instance, malware would cease to be a weapon *per se*, but this does

demonstrate the inherently fuzzy boundaries between which instance of software constitutes a weapon and which does not. "Cyberweapon" is retained here, both because it is tightly if imperfectly defined herein, but also because it provides an opportunity to engage with the substantial literature that already uses the term. It is hoped that future work can develop a more productive and nuanced terminology.

Cyberweapons and global governance

Stuxnet was widely perceived as a "game-changer" in international affairs (Farwell and Rohozinski, 2011, 2012; Collins and McCombie, 2012) by demonstrating the political potential of cyberweapons, which, like all weapons, aim to change the behaviour of an adversary. The reputed subsequent online publication of portions of the Stuxnet code sparked fears of proliferation to non-state actors including terrorists, and the possibility of an inter-state cyber "arms race" (Singer and Friedman, 2014: 158–159; Craig and Valeriano, 2016; Limnéll, 2016). Stuxnet also reinvigorated a long-running discussion about if cyberweapons should be regulated and which parties might be capable of doing so. Early authors on the topic pointed out that non-state use of cyberweapons might be subject to criminal law, and state use by international humanitarian law, but that any regime would be of limited use without significant international commitments to monitoring, verification, compliance and enforcement (Denning, 2000, 2001; Sofaer and Goodman, 2000). States would also be resistant to cyber arms control measures if they restricted their capacity to respond to aggression, by states or non-state actors, although they might help promote norms around offensive cyberweapons use (Eriksson, 1999; Rathmell, 2003).

Subsequent analyses have tended to default to one of two frames in discussing the regulation of cyberweapons. The first is arms control, in which historical experiences with nuclear, biological and chemical weapons serve as resources for thinking through how arms control mechanisms might be applied to cyberweapons (Brown, 2006; Geers, 2010; Meyer, 2011; Arimatsu, 2012; Maybaum and Tölle, 2016). The second frame concerns the criminalization of cyberweapons (Denning, 2000, 2001; Prunckun, 2008), drawing on the evolution of the Council of Europe Convention on Cybercrime (2001), discussed in greater detail below. In both frames, there is a presumption towards globally binding legal mechanisms administered by a central, hierarchical authority and supported by leading powers, the absence of either portending the likely failure of attempts to regulate or prohibit cyberweapons. What is missing from this literature is an attempt to look at cyberweapons governance "in the round", understood as a concern with what currently exists, rather than what might be future optimal solutions (Stevens, 2016b). Specifically, the cyberweapons literature, in its concern with legal and institutional *regimes*, does not address the importance of *global governance* frameworks for understanding international politics.

Emerging at the end of the Cold War and cognisant of the growing potency of globalization, "global governance" represented an interdisciplinary concern with international order in a post-bipolar world (Zumbansen, 2012: 84). In International Relations (IR), this translated into understanding order as having foundations other than traditional political-legal authority, including the roles of transnational and non-state actors, and in finding positive solutions to transnational problems (Hofferberth, 2015: 601). As Coen and Pegram (2015) observe, recent IR global governance scholarship has moved beyond a narrow focus on multilateral institutions and great powers to incorporate the agency of diverse actors and constituencies. One analytical framework emerging from this work is that of "global governance architectures".

A "global governance architecture" is "the overarching system of public and private institutions, principles, norms, regulations, decision-making procedures and organizations that are valid or active in a given issue area of world politics" (Biermann *et al.*, 2009). This framework is narrower in scope than "order", which speaks to the organization of international relations in general, but broader than "regime", which tends towards a focus on institutions (Biermann *et al.*, 2009: 15–16). Global governance architectures consist of vertically fragmented arrangements of multilevel governance (subnational, national, international, supranational) and horizontally fragmented multipolar governance structures of state and non-state actors (Biermann and Pattberg, 2012: 13). The making and implementation of rules is located at multiple points in this matrix, although interlinkages between the various layers and poles of authority and practice are necessary to translate rules and policies from one locus to another. The potential utility of this analytical framework to global cyberweapons governance is currently unexplored. As a first step, the following section identifies existing attempts to regulate cyberweapons in the fields of cyberwarfare, cybercrime, and export controls on dual-use technologies. Each field of activity attempts to regulate a different aspect of cyberweapons acquisition or use. Cyberwarfare is concerned with the use of cyberweapons in war; cybercrime with the acquisition and use of information technologies that can be used in the prosecution of crime by non-state actors; export controls aim to prevent transfer and proliferation of dual-use technologies that can be used to develop or facilitate cyber weapons use by state and non-state actors.

Sources of cyberweapons governance

Cyberwarfare is subject to significant attention presently and one key task is to ascertain how it articulates with international humanitarian law (*jus in bello*). The most comprehensive attempt thus far is the Tallinn Manual Process (TMP), based at the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Estonia. The Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual), an exhaustive analysis by international lawyers, finds that customary international law applies to cyberwarfare, as with other forms of military force (Schmitt, 2013). The Tallinn Manual addresses cyberweapons within this framework, suggesting that they are prohibited from causing "unnecessary suffering" to combatants if military objectives are not furthered by their use (Schmitt, 2013: 143). Non-combatants are already protected in law and should not be subject to cyberweapons use. The TMP has no binding legal status but NATO formally incorporated its recommendations into its Enhanced Cyber Defence Policy (NATO 2014: article 72). The United Kingdom has confirmed these principles in defence strategy (Ministry of Defence, 2013), as has the United States (US Department of Defense, 2015a). US military doctrine for cyberwarfare also respects *opinio juris* on the matter, although submits that "[p]recisely how the law of war applies to cyber operations is not well-settled" (US Department of Defense, 2015b: 996), a situation the second volume of the Tallinn Manual will address in late 2016 (NATO CCD COE, 2015).

Russia asserts that the TMP serves the bellicose interests of "the West", whereas Russia prefers "a diametrically opposed policy of averting military and political confrontations in information space" (Krutskikh and Streltsov, 2014: 75). Both propositions are rejected by one TMP expert, who surmises that Russia criticizes the TMP because it "run[s] counter to their objective of modelling international law in a manner that serves the interests of the

Russian Federation" (von Heinegg, 2015: 2). Neither the Russian claim nor the NATO rebuttal is unjustified: law is as much about facilitation as it is about prohibition. When law is translated into military doctrine, doctrine is an enabler of military operations. It constrains actions in important ways but provides opportunities in others. The TMP and any corresponding processes seek to preserve and maximize military freedom of movement in pursuit of political goals, congruent with particular interpretations of international law and prevailing norms. It follows that the legitimacy and modes of cyberweapons deployment in war depend on how divergent national and coalition interests are translated into laws, norms and, perhaps, future treaties.

The debate about cyberweapons and cyberwarfare rests on the interpretation of existing international law and its applicability to a novel weapons class. In contrast, discussions about global cybercrime have, for the last 15 years, been with principal reference to an entirely new instrument, the Council of Europe Convention on Cybercrime ("Budapest Convention", 2001). The Convention aims to harmonize national cybercrime legislation, enhance transnational policing measures in pursuing and prosecuting cybercriminals, and improve international cybercrime cooperation (Vatis, 2010; Jakobi, 2013: 108–112). The Convention has been signed and ratified by several non-European states, including Canada, Japan, Australia and the United States, and remains open for accession by others. Brazil and India have refused to sign the Convention, as neither played a role in the drafting of the treaty, and Russia claims that transnational policing and investigation violate its sovereignty. China and Russia have suggested that the Shanghai Cooperation Organization is their preferred forum for cybercrime cooperation (Lewis, 2010). Notwithstanding these objections, and issues surrounding its effective implementation (Calderoni, 2010), the Convention is widely regarded as the pre-eminent framework for the prohibition of cybercriminal activities.

The Convention makes no mention of cyberweapons but Article 4.1 requires state parties to criminalize intentional actions in and through computer systems that result in the "damaging, deletion, deterioration, alteration or suppression of computer data without right". Furthermore, state parties may require that such actions "result in serious harm" (Article 4.2). These two articles alone would criminalize the deliberate use of code to cause harm, although the Convention does not further specify to which entities harm must be caused. Article 11 criminalises "aiding and abetting" such activities. There is therefore a range of instances meeting the criteria of intent and harm outlined earlier and the Convention may have further utility in disrupting cyberweapons supply chains. State use of cyberweapons is presumably excepted, although their roles in cyberweapon components markets is legally a grey area and deserves closer attention (Jakobi, 2015; Herzog and Schmid, 2016; Wolf and Fresco, 2016).

The newest source of cyberweapons governance also relies on existing mechanisms, specifically the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996). In December 2013, the Arrangement was extended to classes of hardware and software "specially designed or modified for the generation, operation or delivery of, or communication with 'intrusion software'", defined as software intended to extract or modify data from a computer system or networked device, or which would "allow the execution of externally provided instructions" (Wassenaar Arrangement, 2016). This was the first attempt to incorporate hardware and software associated with cyberweapons into a multilateral regime, although it did not extend to intrusion software itself, into which various cyberweapons components fall. At the end of 2014, EU member-states incorporated the new rules into domestic legislation (Tung, 2014). The United States expressed similar enthusiasm but public consultation revealed significant opposition and in March 2016 the State Department admitted the amendment required renegotiation before translation into domestic law (Barth, 2016). The principal objection was that it would criminalize security researchers using malware systems to improve security products, a potential side-effect recognized since cyberweapons regulation was first discussed (for example, Denning, 2000, 2001). Although "well-intentioned", the amendment would therefore have a negative effect on cybersecurity (Hoffman, 2016).

This indicates clearly the dual-use nature of malware, which can be used for "defensive" and research purposes, as well as "offensive" deployments as cyberweapons proper. In this context, intent determines if malware attains the status of a weapon, not technical considerations (cf. Forge, 2010). It is unclear if the revised Wassenaar Arrangement can be renegotiated to protect legitimate malware uses. Its future efficacy depends on incentivising legitimate security research whilst controlling the export of illegitimate weapons components (Herr, 2016). This task is greatly complicated by Wassenaar's weak enforcement mechanisms, the interplay of state interests, and the technical difficulties in monitoring the transfer of code across the internet (Pyetranker, 2015; Herr, 2016). It does, however, count Russia and the United States as participants, along with 39 other states, which indicates the strength of normative commitments to export controls on dual-use technologies generally.

An emerging global governance architecture

The three fields discussed above—cyberwarfare, cybercrime, export controls—together constitute an emerging global governance architecture for cyberweapons. Each attempts to regulate different aspects of cyberweapons acquisition and use, if not always explicitly in those terms. None is well-advanced institutionally, or in efficacy, as states are still developing cyberweapons and non-state actors still seek to acquire them. Whereas some authors suggest an outright ban on cyberweapons is both possible and desirable (for example, Saran, 2016), the proper frame for considering cyberweapons is regulation, not prohibition. Similarly, whilst ambitions for an overarching treaty framework on cyberweapons are laudable, they founder on well-known obstacles. As Slack (2016: 72) observes of cybersecurity, "the fundamental conception of cyberspace, the lack of a common terminology, the issue of verification, and the dual-use, asymmetric, fast-paced and nonstate-centric nature of the domain … ultimately render a treaty approach unfeasible". Normative approaches are preferred that identify specific issues requiring action, through which "a governance network may emerge where norms of behaviour are developed across a range of fora" (Slack, 2016: 75). One such issue area would be cyberweapons, cooperation over which may be required to settle on "good enough governance" (Grindle, 2004, 2007), rather than aim to close all governance deficits.

This is important because there are significant differences of opinion in all three fields examined here, none of which will be resolved easily but which should not prevent progress being made. Cyberwarfare consensus founders on interpretations of international humanitarian law, particularly as influential *opinio juris* emanates from NATO, to which Russia and China are unsurprisingly resistant. They object similarly to "European" cybercrime initiatives for reasons of sovereignty, which effectively puts two of the world's most important actors outside of the only international convention attempting to regulate cybercrime. The United States objects to the amended Wassenaar Arrangement on the grounds that it undermines security, not that it is seeking to

limit its freedom of action, although that dynamic cannot be discounted. The dispute between "the West" and Russia and China, in particular, portends a return to geopolitics in cyberweapons governance, debates over which express deeper concerns about the nature of security in information environments. As rehearsed many times, there is a difference of opinion at the ideological level between broadly liberal nations that prioritize a global, open internet and more authoritarian regimes that seek to regulate the internet along national lines, although liberal states are not exempt from accusations of naked self-interest (Mueller, 2010; DeNardis, 2014; Carr, 2015; Powers and Jablonski, 2015). On the credit side of the ledger, however, there is significantly more cooperation within these fields at present than there has ever been.

Conclusion

This commentary has introduced the concept of cyberweapons governance but is under no illusions that such a discrete policy field currently exists in any formal sense. It does not. It is merely a suggestion that more attention to this issue is required, particularly as practice evolves rapidly and secondary analyses proliferate. As a first step, it has described where cooperation and conflict exist between institutions, norms and major actors, and some of the reasons why. It would also be productive to consider the precise institutional and processual paths by which each of these architectural components has come to exist, as such historical considerations are beyond the scope of this article. The evidence base at present favours analyses of state and inter-governmental initiatives but more research is also required into the actions of civil society, industry and other non-state actors. This would reflect scholarly work on global cybersecurity and internet governance more broadly, which overlaps with some of the concerns raised in this article in both theory and practice (Mueller, 2010; DeNardis, 2014; Nye, 2014; Saran, 2016.

One final suggestion is that fragmentation is inherent to global governance architectures and should not be considered an *a priori* impediment to global cyberweapons governance. This is in contrast to most work on cyberweapons, which presents fragmentation as the antithesis of progress. Instead, fragmentation should be viewed as inevitable and, to a certain extent, as an opportunity. Efforts should be directed towards reducing conflicts over norms and institutions, rather than convergent norms and hierarchical institutions being viewed as prerequisites for effective governance.

Cyberweapons governance is a problematic proposition, on account of environmental complexity; monitoring, verification, compliance and enforcement; and, power politics. The diversity of actors and institutions is also a major challenge but may be its strength. Regulatory innovation emerges not through hierarchies but through diversity. The plethora of public-private partnerships, bilateral agreements, memoranda of understanding, industry initiatives, confidence-building measures and civil society activism, in the broad field of cyber security may encourage the development of novel technical, political and organizational proposals contributing to workable and effective cyberweapons governance. Cyberweapons governance is a daunting prospect but one that needs to be addressed as an emerging security issue. In this respect, fragmentation should be regarded as a condition of progress and as a reaction to the "fuzziness" of the object of governance itself, not as a sign of failure or an excuse for inaction. It took many years to develop effective frameworks for regulating and prohibiting other weapons classes (Mazanec, 2015). None is perfect but each serves the public good better than its absence. So too with cyberweapons. Their full capabilities have yet to be demonstrated but cyberweapons may in future cause substantial harm and damage, maybe even to human life itself. A global governance architecture for cyberweapons is developing quietly and haltingly. It is fragmented and contested but perhaps more constructive than none at all.

References

Arimatsu L (2012) A treaty for governing cyber-weapons: potential benefits and practical limitations. In: Czosseck C, Ottis R and Ziolkowski K (eds). *Proceedings of the 4th International Conference on Cyber Conflict, Tallinn, Estonia, 5–8 June*. CCD COE Publications: Tallinn, pp 91–109.

Barth B (2016) Executive branch concedes Wassenaar Arrangement must be renegotiated, not revised. *SC Magazine* 3 March, http://www.scmagazine.com/executive-branch-concedes-wassenaar-arrangement-must-be-renegotiated-not-revised/article/481020/.

Barzashka I (2013) Are cyber-weapons effective? *The RUSI Journal*; **158** (2): 48–56.

Biermann F and Pattberg P (2012) Global environmental governance revisited In: Biermann F and Pattberg P (eds). *Global Environmental Governance Reconsidered*. The MIT Press: Cambridge, MA, pp 1–23.

Biermann F, Pattberg P, van Asselt H and Zelli F (2009) The fragmentation of global governance architecture: a framework for analysis. *Global Environmental Politics*; **9** (4): 14–40.

Boothby B (2016) Cyber weapons: Oxymoron or a real world phenomenon to be regulated? In: Friis K and Ringsmose J (eds). *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. Routledge: Abingdon, UK; New York, pp 165–174.

Bourne M (2012) Guns don't kill people, cyborgs do: a Latourian provocation for transformatory arms control and disarmament. *Global Change, Peace & Security*; **24** (1): 141–163.

Brown D (2006) A proposal for an international convention to regulate the use of information systems in armed conflict. *Harvard International Law Journal*; **47** (1): 179–221.

Calderoni F (2010) The European legal framework on cybercrime: striving for an effective implementation. *Crime, Law & Social Change*; **54** (5): 339–357.

Carr M (2015) Power plays in global internet governance. *Millennium: Journal of International Studies*; **43** (2): 640–659.

Coen D and Pegram T (2015) Wanted: a third generation of global governance research. *Governance*; **28** (4): 417–420.

Collins S and McCombie S (2012) Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence & Counter Terrorism*; **7** (1): 80–91.

Craig A and Valeriano B (2016) Conceptualising cyber arms races. In: Pissanidis N, Rõigas H and Veenendaal M (eds). *Proceedings of the 8th International Conference on Cyber Conflict: Cyber Power, Tallinn, Estonia, 31 May-3 June*. CCD COE Publications: Tallinn, pp 141–58.

DeNardis L (2014) *The Global War for Internet Governance*. Yale University Press: New Haven, CT.

Denning DE (2000) Reflections on cyberweapons controls. *Computer Security Journal*; **16** (4): 43–53.

Denning DE (2001) Obstacles and options for cyber arms control. Paper presented at *Arms Control in Cyberspace: Perspectives for Peace Policy in the Age of Computer Network Attacks* conference, Berlin, 29–30 June.

Dipert RR (2014) The essential features of an ontology for cyberwarfare In: Yannakogeorgos PA and Lowther AB (eds). *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Taylor and Francis: Boca Raton, FL, pp 35–48.

Eriksson EA (1999) Viewpoint: Information warfare: hype or reality? *The Nonproliferation Review*; **6** (3): 57–64.

Farwell JP and Rohozinski R (2011) Stuxnet and the future of cyber war. *Survival*; **53** (1): 23–40.

Farwell JP and Rohozinski R (2012) The new reality of cyber war. *Survival*; **54** (4): 107–120.

Floridi L (2014) The latent nature of global information warfare. *Philosophy & Technology*; **27** (3): 317–319.

Forge J (2010) A note on the definition of 'dual use'. *Science & Engineering Ethics*; **16** (1): 111–118.

Geers K (2010) Cyber weapons convention. *Computer Law & Security Review*; **26** (5): 547–551.

Grindle MS (2004) Good enough governance: poverty reduction and reform in developing countries. *Governance*; **17** (4): 525–548.

Grindle MS (2007) Good enough governance revisited. *Development Policy Review*; **25** (4): 553–574.

Herr T (2016) Malware counter-proliferation and the Wassenaar Arrangement. In: Pissanidis N, Rõigas H and Veenendaal M (eds). *Proceedings of the 8th International Conference on Cyber Conflict: Cyber Power, Tallinn, Estonia, 31 May-3 June*. CCD COE Publications: Tallinn, pp 175–190.

Herzog M and Schmid J (2016) Who pays for zero-days? Balancing long-term stability in cyber space against short-term national security benefits In: Friis K and Ringsmose J (eds). *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. Routledge: Abingdon, UK; New York, pp 95–115.
Hofferberth M (2015) Mapping the meanings of global governance: a conceptual reconstruction of a floating signifier. *Millennium: Journal of International Studies*; **43** (2): 598–617.
Hoffman KE (2016) Unsuitable addendum: Wassenaar Arrangement. *SC Magazine* 9 May, https://www.scmagazine.com/unsuitable-addendum-wassenaar-arrangement/article/530284/.
Jakobi AP (2013) *Common Goods or Evils? The Formation of Global Crime Governance*. Oxford University Press: Oxford.
Jakobi AP (2015) From prohibition to regulation? The global governance of illegal markets. Paper presented at the *Comparing the Global Governance of Illegal Markets* workshop, October, Bielefeld, Germany.
Krutskikh A and Streltsov A (2014) International law and the problem of international information security. *International Affairs [Mezdunarodnaia zhizn]*; **60** (6): 64–76.
Lewis JA (2010) Multilateral agreements to constrain cyberconflict. *Arms Control Today*; **40** (5): 14–19.
Limnéll J (2016) The cyber arms race is accelerating: what are the consequences? *Journal of Cyber Policy*; **1** (1): 50–60.
Linklater A (2006) The harm principle and global ethics. *Global Society*; **20** (3): 329–343.
Maybaum M and Tölle J (2016) Arms control in cyberspace: architecture for a trust-based implementation framework based on conventional arms control methods. In: Pissanidis N, Rõigas H and Veenendaal M (eds). *Proceedings of the 8th International Conference on Cyber Conflict: Cyber Power, Tallinn, Estonia, 31 May-3 June*. CCD COE Publications: Tallinn, pp 159–173.
Mazanec BM (2015) *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. Potomac Books: Lincoln, NE.
Mele S (2013) *Cyber-Weapons: Legal and Strategic Aspects*; version 2.0, June Italian Institute of Strategic Studies: Rome, Italy.
Meyer P (2011) Cyber-security through arms control: an approach to international co-operation. *The RUSI Journal*; **156** (2): 22–27.
Ministry of Defence. (2013) *Cyber Primer*. Ministry of Defence: London.
Mueller ML (2010) *Networks and States: The Global Politics of Internet Governance*. The MIT Press: Cambridge, MA.
NATO. (2014) Wales Summit Declaration. Press release, 5 September, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.
NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). (2015) Tallinn Manual 2.0 to be completed in 2016. Press release, 9 October, https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html.
Nye JS Jr (2014) *The Regime Complex for Managing Global Cyber Activities*. Global Commission on Internet Governance Paper Series 1. Global Commission on Internet Governance: Waterloo, ON and Chatham House: London.
Powers SM and Jablonski M (2015) *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press: Urbana, Chicago and Springfield, IL.
Prunckun H (2008) 'Bogies in the wire': Is there a need for legislative control of cyber weapons? *Global Crime*; **9** (3): 262–272.
Pyetranker I (2015) An umbrella in a hurricane: Cyber technology and the December 2013 amendment to the wassenaar arrangement. *Northwestern Journal of Technology & Intellectual Property*; **13** (2): 153–180.
Rathmell A (2003) Controlling computer network operations. *Studies in Conflict & Terrorism*; **26** (3): 215–232.
Rid T (2013) *Cyber War Will Not Take Place*. Hurst & Company: London.
Rid T and McBurney P (2012) Cyber-weapons. *The RUSI Journal*; **157** (1): 6–13.
Sanger DE (2012) *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Crown Publishers: New York.
Saran S (2016) Striving for an international consensus on cyber security: lessons from the 20th century. *Global Policy*; **7** (1): 93–95.
Schmitt MN (ed) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press: Cambridge, UK.
Singer PW and Friedman A (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press: New York.
Slack C (2016) Wired yet disconnected: the governance of international cyber relations. *Global Policy*; **7** (1): 69–78.
Sofaer AD and Goodman SE (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*. Working paper. Stanford University: Stanford, CA.
Stevens T (2016a) *Cyber Security and the Politics of Time*. Cambridge University Press: Cambridge, UK.
Stevens T (2016b) Cyberweapons: governing the ungovernable? *Political Studies Association* blog, 28 June, https://www.psa.ac.uk/insight-plus/blog/cyberweapons-governing-ungovernable.
Tung L (2014) EU exploit vendors will need a 'licence to sell' from 31 December. *CSO Online*, 19 December, http://www.cso.com.au/article/562845/eu-exploit-vendors-will-need-licence-sell-from-31-december/.
US Department of Defense. (2015a) *Cyber Strategy*. Department of Defense: Washington DC.
US Department of Defense. (2015b) *Law of War Manual*. Office of General Counsel, Department of Defense: Washington DC.
Valeriano B, Roff H and Lawson S (2016) Dropping the cyber bomb? Spectacular claims and unremarkable effects. *Council on Foreign Relations* blog, 24 May, http://blogs.cfr.org/cyber/2016/05/24/dropping-the-cyber-bomb-spectacular-claims-and-unremarkable-effects/.
Vatis MA (2010) The Council of Europe Convention on Cybercrime. In: *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy, 10–11 June, Washington, DC.* The National Academies Press: Washington DC, pp 207–223.
von Heinegg WH (2015) *International Law and International Information Security: A Response to Krutskikh and Streltsov*. Tallinn Paper no. 9. CCD COE Publications: Tallinn.
Wassenaar Arrangement. (2016) *List of Dual-Use Goods and Technologies and Munitions List*. WA-LIST (15) 1 Corr. 1, 4 April, http://www.wassenaar.org/wp-content/uploads/2016/04/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf..
Wolf MJ and Fresco N (2016) Ethics of the software vulnerabilities and exploits market. *The Information Society: An International Journal*; **32** (4): 269–279.
Zetter K (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishers: New York.
Zumbansen P (2012) Governance: an interdisciplinary perspective In: Levi-Faur D (ed). *The Oxford Handbook of Governance*. Oxford University Press: Oxford, pp 83–96.

Acknowledgements

Versions of this article were presented at Royal Holloway, University of London, March 2016; British International Studies Association annual conference, Edinburgh, June 2016; and, UCL Global Governance Institute, June 2016. I am grateful to all participants for their comments and suggestions.

Additional information

Competing interests: The Authors declare no competing financial interests.

Reprints and permission information is available at http://www.palgrave-journals.com/pal/authors/rights_and_permissions.html

How to cite this article: Stevens T (2016) Cyberweapons: an emerging global governance architecture. *Palgrave Communications*. 2:160102 doi: 10.1057/palcomms.2016.102.